CLAIMS

1. (Original) A subscriber identification module for providing local authentication of a subscriber in a communication system, comprising:

a memory; and

a processor configured to implement a set of instructions stored in the memory, the set of instructions for:

generating a plurality of keys in response to a received challenge;

generating an initial value based upon a first key from the plurality of keys;

concatenating the initial value with a received signal to form an input value, wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit;

hashing the input value to form an authentication signal; and

transmitting the authentication signal to the communications system via the communications unit.

2. (Original) The apparatus of Claim 1, wherein hashing the input value is performed in accordance with the Secure Hashing Algorithm (SHA-1).

3. (Original) The apparatus of Claim 1, wherein generating the initial value comprises padding the first key.

4. (Original) The apparatus of Claim 3, wherein generating the initial value further comprises adding the padded first key bit-wise to a constant value.

5. (Original) The apparatus of Claim 1, wherein the received signal is generated at the communications unit by:

receiving the second key from the subscriber identification module;

generating a local initial value based upon the second key;

concatenating the local initial value and a message to form a local input value;

hashing the local input value to form the received signal; and

transmitting the received signal to the subscriber identification module.

6. (Original) The apparatus of Claim 5, wherein generating the local initial value comprises padding the second key.

7. (Original) The apparatus of Claim 6, wherein generating the local initial value further comprises adding the padded second key bit-wise to a second constant value.

8. (Original) A subscriber identification module, comprising:

a key generation element; and

a signature generator configured to receive a secret key from the key generation element and information from a mobile unit, and further configured to generate a signature that will be

sent to the mobile unit, wherein the signature is generated by concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information.

9. (Original) The subscriber identification module of Claim 8, wherein the key generation element comprises:

a memory; and

a processor configured to execute a set of instructions stored in the memory, wherein the set of instructions performs a cryptographic transformation upon an input value to produce a plurality of temporary keys.

10. (Original) The subscriber identification module of Claim 9, wherein the cryptographic transformation is performed using a permanent key.

11. (Original) An apparatus for providing secure local authentication of a subscriber in a communication system, comprising a subscriber identification module configured to interact with a communications unit, wherein the subscriber identification module comprises:

a key generator for generating a plurality of keys from a received value and a secret value, wherein at least one communication key from the plurality of keys is delivered to the communications unit and at least one secret key from the plurality of keys is not delivered to the communications unit; and

a signature generator for generating an authorization signal from hashing a version of the at least one secret key together with an authorization message, wherein the authorization message is generated by the communications unit using a version of the at least one communication key.

12. (Original) The apparatus of Claim 11, wherein the subscriber identification module is configured to be inserted into the communications unit.

13. (Original) The apparatus of Claim 11, wherein the at least one communication key comprises an integrity key.

14. (Original) The apparatus of Claim 11, wherein hashing is performed in accordance with SHA-1.

15. (Original) A method for providing authentication of a subscriber using a subscriber identification device, comprising:

generating a plurality of keys;

transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys;

generating a signature at the communications device using both the at least one key transmitted to the communications device and a transmission message, wherein generating is implemented by hashing a concatenated value formed from the at least one key and the transmission message;

transmitting the signature to the subscriber identification device;

receiving the signature at the subscriber identification device;

generating a primary signature from the received signature, wherein the generating is implemented by hashing a concatenated value formed from the at least one private key and the signature received from the communications device; and

conveying the primary signature to a communications system.

16. (Original) The method of Claim 15, wherein hashing is implemented in accordance with SHA-1.

17. (Previously Presented) An apparatus for authenticating a subscriber in a wireless communication system, wherein the apparatus can be communicatively coupled to a mobile station operating within the wireless communications system, comprising:

a memory; and

a processor configured to implement a set of instructions stored in the memory, the set of instructions for selectively generating a primary signature based upon a key that is held private from the mobile station and a secondary signature that is received from the mobile station, wherein the primary signature is conveyed to the mobile station for authenticating the subscriber.

18. (Previously Presented) A method operational on a subscriber identification device for providing local authentication of a subscriber, comprising:

generating a plurality of keys in response to a received challenge;

generating an initial value based on a first key from the plurality of keys;

concatenating the initial value with a received signal to form an input value, wherein the received signal is transmitted from a communications unit communicatively coupled to the

subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit;

hashing the input value to form an authentication signal; and

transmitting the authentication signal to the communications system via the communications unit.

19. (Previously Presented) A subscriber identification module for providing local authentication of a subscriber in a communication system, comprising:

means for generating a plurality of keys in response to a received challenge;

means for generating an initial value based on a first key from the plurality of keys;

means for concatenating the initial value with a received signal to form an input value, wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit;

means for hashing the input value to form an authentication signal; and

means for transmitting the authentication signal to the communications system via the communications unit.

20. (Previously Presented) A machine-readable medium having one or more instructions for authenticating a subscriber using a subscriber identification device, which when executed by a processor causes the processor to:

generate a plurality of keys in response to a received challenge;

generate an initial value based on a first key from the plurality of keys;

concatenate the initial value with a received signal to form an input value, wherein the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module, and the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit;

hash the input value to form an authentication signal; and

transmit the authentication signal to the communications system via the communications unit.

21. (Previously Presented) A method operational on a subscriber identification device, comprising:

receiving a secret key from a key generation element and information from a mobile unit;

concatenating the secret key with the information from the mobile unit;

hashing the concatenated secret key and information to generate a signature; and

sending the signature to the mobile unit.

22. (Previously Presented) The method of claim 21 further comprising:

performing a cryptographic transformation on an input value to produce a plurality of temporary keys.

23. (Previously Presented) A subscriber identification device, comprising:

means for receiving a secret key from a key generation element and information from a mobile unit;

means for concatenating the secret key with the information from the mobile unit;

means for hashing the concatenated secret key and information to generate a signature; and

means for sending the signature to the mobile unit.

24. (Previously Presented) The method of claim 23 further comprising:

means for performing a cryptographic transformation on an input value to produce a plurality of temporary keys.

25. (Previously Presented) A machine-readable medium having one or more instructions operational on a subscriber identification device for authenticating a subscriber, which when executed by a processor causes the processor to:

receive a secret key from a key generation element and information from a mobile unit;

concatenate the secret key with the information from the mobile unit;

hash the concatenated secret key and information to generate a signature; and

send the signature to the mobile unit.

26. (Previously Presented)The machine-readable medium of claim 25 further having one or more instructions which when executed by a processor causes the processor to:

perform a cryptographic transformation on an input value to produce a plurality of temporary keys.

27. (Previously Presented)A method operational on a subscriber identification module for providing secure local authentication of a subscriber in a communication system, comprising:

generating a plurality of keys from a received value and a secret value;

delivering at least one communication key from the plurality of keys to a communication unit configured to interact with the subscriber identification module;

withholding at least one secret key from the plurality of keys from the communication unit; and

hashing a version of the at least one secret key together with an authorization message to generate an authorization signal, wherein the authorization message is generated by the communications unit using a version of the at least one communication key.

28. (Previously Presented)A subscriber identification module for providing secure local authentication of a subscriber in a communication system, comprising:

means for generating a plurality of keys from a received value and a secret value;

means for delivering at least one communication key from the plurality of keys to a communication unit configured to interact with the subscriber identification module;

means for withholding at least one secret key from the plurality of keys from the communication unit; and

means for hashing a version of the at least one secret key together with an authorization message to generate an authorization signal, wherein the authorization message is generated by the communications unit using a version of the at least one communication key.

29. (Previously Presented) A machine-readable medium having one or more instructions operational on a subscriber identification device for providing secure local authentication of a subscriber in a communication system, which when executed by a processor causes the processor to:

generate a plurality of keys from a received value and a secret value;

deliver at least one communication key from the plurality of keys to a communication unit configured to interact with the subscriber identification module;

withhold at least one secret key from the plurality of keys from the communication unit; and

hash a version of the at least one secret key together with an authorization message to generate an authorization signal, wherein the authorization message is generated by the communications unit using a version of the at least one communication key.

30. (Previously Presented) A method operational on a device for authenticating a subscriber in a wireless communication system, comprising:

receiving a secondary signature from a mobile station operating within the wireless communications system, wherein the device is configured to be communicatively coupled to the mobile station; and

generating a primary signature based on a key that is held private from the mobile station and the secondary signature, wherein the primary signature is conveyed to the mobile station for authenticating the subscriber.

31. (Previously Presented) A device for authenticating a subscriber in a wireless communication system, comprising:

means for receiving a secondary signature from a mobile station operating within the wireless communications system, wherein the device is configured to be communicatively coupled to the mobile station; and

means for generating a primary signature based on a key that is held private from the mobile station and the secondary signature, wherein the primary signature is conveyed to the mobile station for authenticating the subscriber.

32. (Previously Presented) A machine-readable medium having one or more instructions operational on a device for authenticating a subscriber in a wireless communication system, which when executed by a processor causes the processor to:

receiving a secondary signature from a mobile station operating within the wireless communications system, wherein the device is configured to be communicatively coupled to the mobile station; and

generating a primary signature based on a key that is held private from the mobile station and the secondary signature, wherein the primary signature is conveyed to the mobile station for authenticating the subscriber.